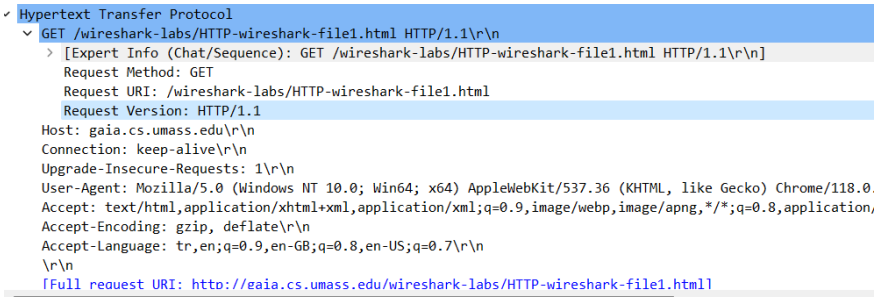
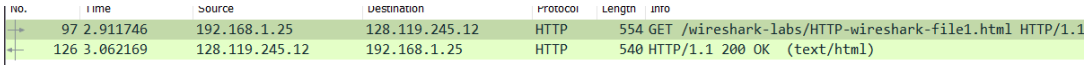
WSA2 - HTTP

1



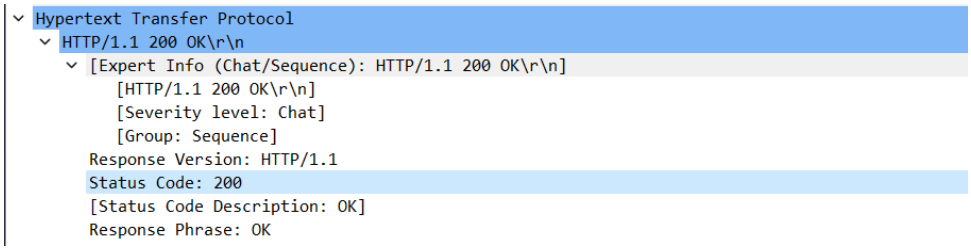
Version: 1.1

Languages: tr, en, en-gb, en-us



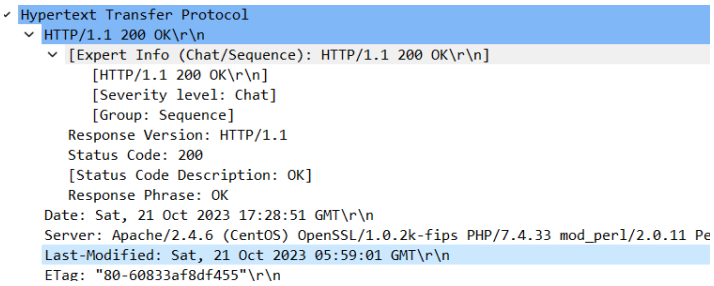
Ip address of my computer: 192.168.1.25

Ip address of http server: 128.119.245.12



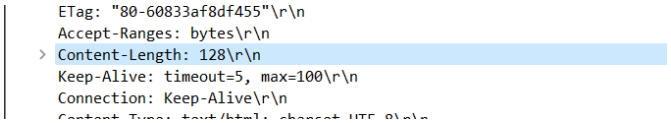
Status code: 200

Status phrase: OK



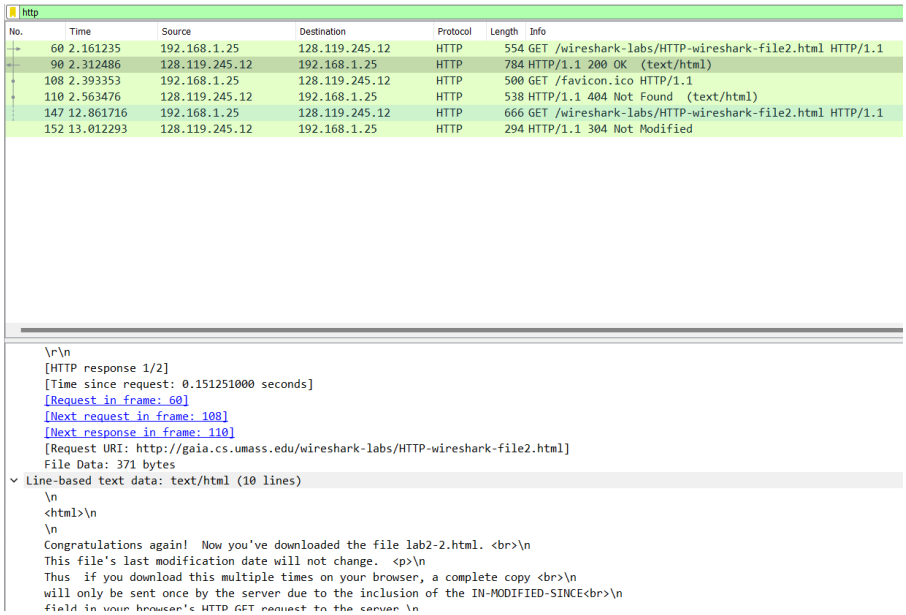
Date: 10/21/2023

Time: 05:59:01



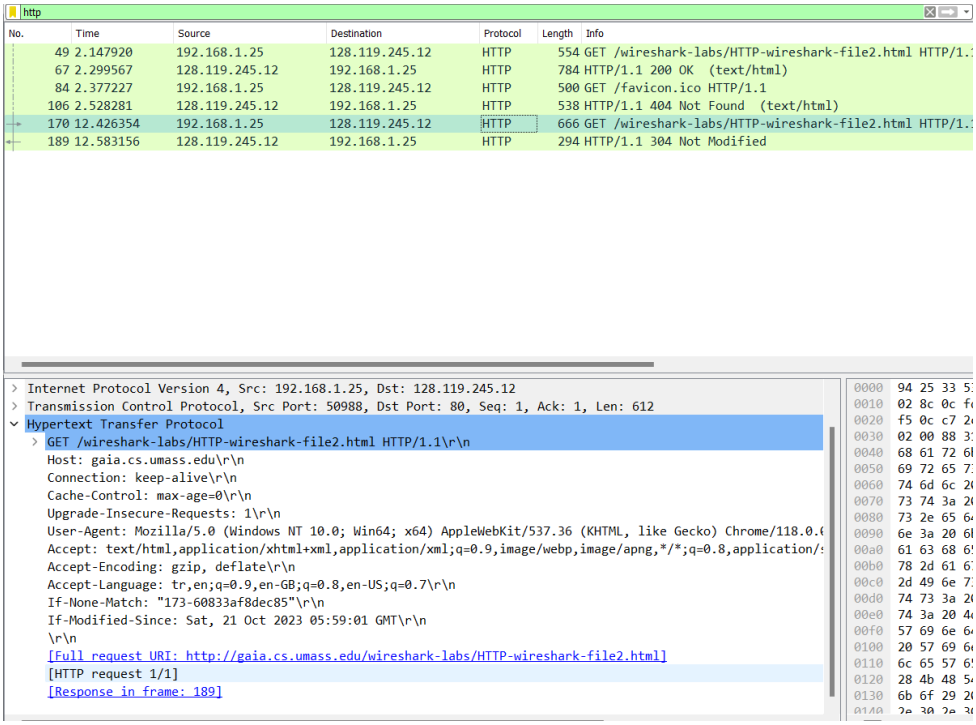
128 bytes of content are being returned to my browser.

2



The first HTTP GET request does not contain “if-modified-since” line.

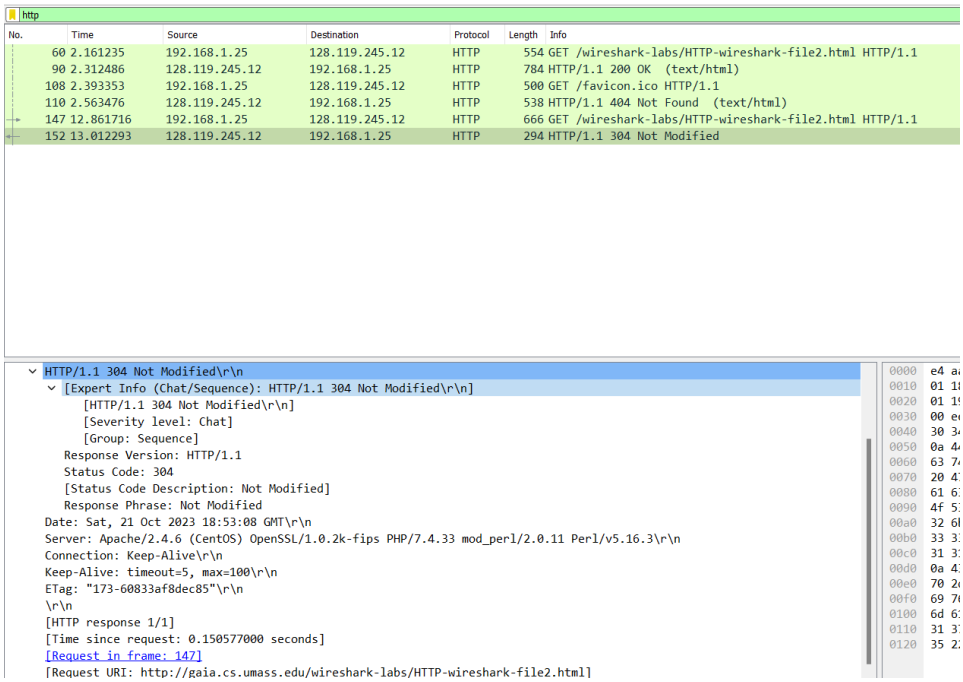
The server returned full contents of file in 200 OK reply message.



The second HTTP GET request contains “If-Modified-Since” line.

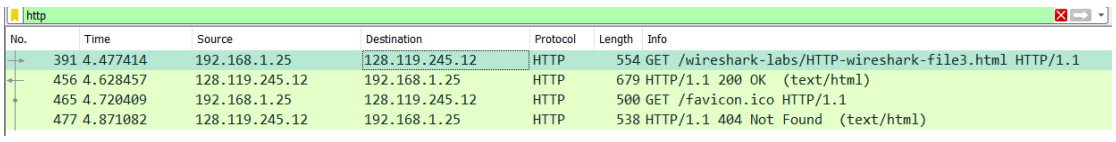
```
   Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
If-None-Match: "173-60833af8dec85"\r\n
If-Modified-Since: Sat, 21 Oct 2023 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 152]
```

A date and time stamp.



The server did not return the full contents of file with “304 Not Modified” reply message.

3



My browser sent 1 request message in order to download the lengthy US Bill of Rights and its packet number is 391. The server replied it with status code 200 and status phase OK on packet number 456.

```
> Frame 456: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface \Device\NPF_{DC50A74E-
> Ethernet II, Src: HuaweiTe_53:78:6a (94:25:33:53:78:6a), Dst: LiteonTe_e0:ed:b3 (e4:aa:ea:e0:ed:b3)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.25
> Transmission Control Protocol, Src Port: 80, Dst Port: 51477, Seq: 4237, Ack: 501, Len: 625
> [4 Reassembled TCP Segments (4861 bytes): #453(1412), #454(1412), #455(1412), #456(625)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 21 Oct 2023 20:25:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

4 TCP segments.

4

http

No.	Time	Source	Destination	Protocol	Length	Info
556	3.423883	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/
598	3.574333	128.119.245.12	192.168.1.25	HTTP	1355	HTTP/1.1 200 OK (text/html)
612	3.593310	192.168.1.25	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
648	3.737238	192.168.1.25	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
651	3.744967	128.119.245.12	192.168.1.25	HTTP	841	HTTP/1.1 200 OK (PNG)
663	3.802455	178.79.137.164	192.168.1.25	HTTP	225	HTTP/1.1 301 Moved Permanently
722	4.103381	192.168.1.25	212.252.126.88	HTTP	372	GET /roots/dstrootcax3.p7c HTTP/1.1
728	4.114545	212.252.126.88	192.168.1.25	HTTP	1460	HTTP/1.1 200 OK
1267	4.591470	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
1290	4.742416	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

4 HTTP GET request messages.

http

No.	Time	Source	Destination	Protocol	Length	Info
556	3.423883	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
598	3.574333	128.119.245.12	192.168.1.25	HTTP	1355	HTTP/1.1 200 OK (text/html)
612	3.593310	192.168.1.25	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
648	3.737238	192.168.1.25	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
651	3.744967	128.119.245.12	192.168.1.25	HTTP	841	HTTP/1.1 200 OK (PNG)
663	3.802455	178.79.137.164	192.168.1.25	HTTP	225	HTTP/1.1 301 Moved Permanently
722	4.103381	192.168.1.25	212.252.126.88	HTTP	372	GET /roots/dstrootcax3.p7c HTTP/1.1
728	4.114545	212.252.126.88	192.168.1.25	HTTP	1460	HTTP/1.1 200 OK
1267	4.591470	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
1290	4.742416	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

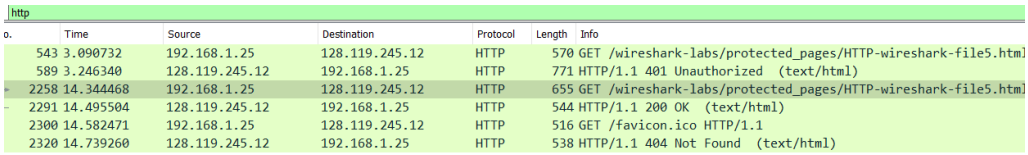
Exactly two different HTTP GET request went to 128.119.245.12 on 556 and 612. One additional http GET request went to 178.79.137.164 and it returns 301 Object moved code. So, fourth one went to 212.252.126.88.

5

http

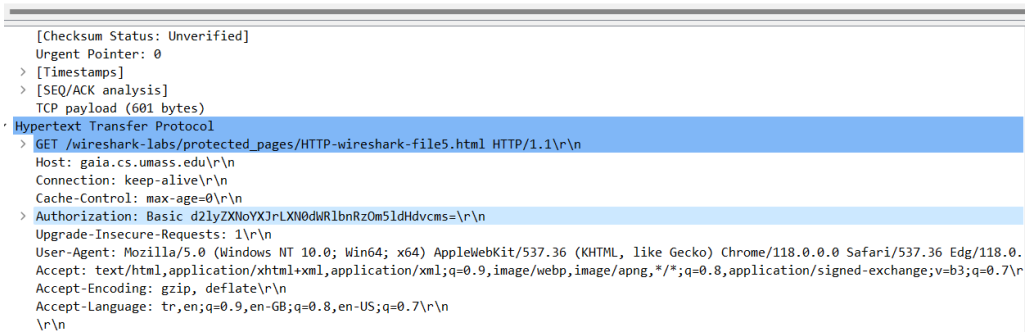
o.	Time	Source	Destination	Protocol	Length	Info
543	3.090732	192.168.1.25	128.119.245.12	HTTP	570	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
589	3.246340	128.119.245.12	192.168.1.25	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2258	14.344468	192.168.1.25	128.119.245.12	HTTP	655	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2291	14.495504	128.119.245.12	192.168.1.25	HTTP	544	HTTP/1.1 200 OK (text/html)
2300	14.582471	192.168.1.25	128.119.245.12	HTTP	516	GET /favicon.ico HTTP/1.1
2320	14.739260	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet number of the first HTTP GET request is 543. The server's response is 401 Unauthorized.



http

o.	Time	Source	Destination	Protocol	Length	Info
543	3.090732	192.168.1.25	128.119.245.12	HTTP	570	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
589	3.246340	128.119.245.12	192.168.1.25	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2258	14.344468	192.168.1.25	128.119.245.12	HTTP	655	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
2291	14.495504	128.119.245.12	192.168.1.25	HTTP	544	HTTP/1.1 200 OK (text/html)
2300	14.582471	192.168.1.25	128.119.245.12	HTTP	516	GET /favicon.ico HTTP/1.1
2320	14.739260	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)



```
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (601 bytes)
Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 Edg/118.0.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
    \r\n
```

Authorization field is included in the second HTTP GET message.